UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,320	03/26/2001	Barry Lynn Royer	2001P04781US	8856

7590   09/09/2004

Siemens Corporation
Intellectual Property Department
186 Wood Avenue South
Iselin, NJ 08830

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

> A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
> THE MAILING DATE OF THIS COMMUNICATION.
> - Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
>   after SIX (6) MONTHS from the mailing date of this communication.
> - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
> - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
> - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
>   Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
>   earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _26 March 2001_.

2a)☐ This action is **FINAL.** 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-22_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _20010412, 20030131_.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2.   Claim 12 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for encryption using triple DES, does not reasonably provide enablement for encryption using the RSA algorithm. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to use the invention commensurate in scope with these claims. Disclosure of the use of triple DES does not sufficiently enable or justify the use of RSA, as triple DES is a symmetric encryption algorithm, while RSA is an asymmetric encryption algorithm. It would not be possible to substitute an asymmetric algorithm for a symmetric algorithm without performing modifications. It is acknowledged that Applicant refers to the RSA MD5 hashing algorithm; however, as the Claim refers to encryption using the RSA algorithm, it appears that this is not in reference to MD5. For the purpose of applying the prior art, it has been assumed that the claim refers to the RSA encryption algorithm and not to triple DES.

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

Claim 2 recites the limitation "data either lying between 'http://' and a

question mark '?' or from data lying between 'http://' and a pound/number sign '#'

– whichever comes first" in lines 15-17. It is unclear whether "whichever comes

first" refers to whichever is first of the data between the "http://" and the question

mark and the data between the "http://" and the pound sign, or to whichever is

first of the question mark and the pound sign. This renders the claim indefinite.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section
> 122(b), by another filed in the United States before the invention by the applicant for patent or
> (2) a patent granted on an application for patent by another filed in the United States before
> the invention by the applicant for patent, except that an international application filed under
> the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an
> application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

6.   Claims 1-11, 13-22 are rejected under 35 U.S.C. 102(e) as being

anticipated by Calamera et al, US Patent 6463533.

In reference to Claim 1, Calamera discloses a system including a link

processor (Figure 2, ALIAS generation server system 30) that identifies and

encrypts an address portion of a URL (DOMAIN and PATH of column 8, lines 43-

48) and incorporates the encrypted address portion with the non-encrypted

portion and a communication processor that incorporates the processed URL

data into formatted data (ALIAS of column 8, lines 58-60).

In reference to Claims 2, 3, and 4, Calamera further discloses adaptively

identifying the address portion (column 7, lines 32-34).

In reference to Claims 5 and 7, Calamera further discloses compressing

the address portion prior to encryption using a hash function (MD5, see column

8, lines 48-50).

In reference to Claim 6, Calamera further discloses converting the address

portion (column 8, lines 48-52).

In reference to Claims 8 and 9, Calamera further discloses incorporating a

session identifier into the processed URL data by formatting the identifier

(column 8, lines 52-58).

In reference to Claim 10, Calamera further discloses concatenating the

address portion with data associated with a personal record to form a data

element and encrypting the data element (ID of column 8, lines 56-58).

In reference to Claim 11, Calamera further discloses that the personal

record data is a user identifier (ID, as defined in column 7, lines 35-36).

In reference to Claims 13 and 14, Calamera discloses a system including a link processor (Figure 2, ALIAS generation server system 30) that identifies an address portion of a URL; compresses, using a hash function, the address portion (DOMAIN and PATH of column 8, lines 48-50); encrypts the compressed address portion (column 8, lines 43-48); and incorporates the encrypted address portion with the non-encrypted portion. Calamera further discloses a communication processor that incorporates the processed URL data into formatted data (ALIAS of column 8, lines 58-60).

In reference to Claim 15, Calamera discloses a system including an input processor for receiving an encoded URL (column 9, lines 20-23), a link processor (Figure 3, Alias server system 42) that identifies an encrypted address portion of the received URL and decrypts the encrypted address portion (column 9, lines 24-26), and a validation processor (Figure 3, Alias server system 42) that determines if the decrypted address portion has been subject to unauthorized modification (column 9, lines 29-31).

In reference to Claim 16, Calamera further discloses applying a hash function to a URL corresponding to the encoded URL and comparing the first and second hash values to determine if validation of the received URL is successful (column 9, lines 26-31).

In reference to Claim 17, Calamera further discloses a session identifier (column 8, lines 52-58).

In reference to Claim 18, Calamera further discloses data associated with a personal record (ID, column 8, lines 56-58).

In reference to Claim 19, Calamera further discloses that the personal record data is a user identifier (ID, as defined in column 7, lines 35-36).

Claim 20 is directed to a method that corresponds substantially to the system of Claim 1, and is rejected by a similar rationale.

Claim 21 and 22 are directed to methods that correspond substantially to the systems of Claims 15 and 16, and are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Calamera et al, US Patent 6463533, in view of Schneier, *Applied Cryptography*.

Calamera discloses everything as applied to Claim 1 above. Calamera does not explicitly disclose the use of the RSA algorithm in encryption. However, Calamera does disclose that a public key encryption algorithm could be used with modifications to the disclosed system (column 9, lines 46-48). Schneier

discloses that the RSA algorithm is a well-known public key algorithm that can be used for both encryption and digital signatures (page 17, section 1.6, "Computer Algorithms"). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Calamera to use the RSA algorithm for performing the encryption, to take advantage of both its ease of use and the fact that the algorithm has withstood extensive cryptanalysis (see Schneier, pages 466-467, section 19.3, "RSA").

Conclusion

9.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a.   Levergood et al, US Patent 5708780, disclose an access control system including a URL containing a hash of an encrypted session identifier.

b.   Reiche, US Patent 6092196, discloses a user authentication system that includes encoding and encrypting identifying information into a URL.

c.   Ruben et al, US Patent 6138237, disclose a system for protecting access to network resources including encrypted and hashed certificate URLs.

d.   Dias et al, US Patent 6170017, disclose a method and system that performs user authentication and uses encrypted session IDs in URLs.

e.   Moore et al, US Patent 6330575, disclose a method and system for developing web pages that includes encrypted information in URLs.

f.   Schmeidler et al, US Patent 6374402, disclose a secure content delivery system including a launch string that is compressed and encrypted to form a processed URL.

g.   Todd, US Patent 6463418, discloses a transaction system that includes encrypted transaction information in URLs.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870, as of October 2004. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).

zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137